ABSTRACT

A data encryption system implemented by running on a cache-equipped computer an encryption program including transformation tables each of which contains a predetermined number of entries. All or necessary ones of the transformation tables are loaded into the cache memory before encryption/decryption process. This causes encryption/decryption time to be made substantially equal independently of the number of operation entries for the transformation table. It is very difficult to extract plain texts used to determine a key differential, resulting in difficulties in cryptanalysis.